(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
26 June 2014 (26.06.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/100788 A3

(51) International Patent Classification:
H04L 9/00 (2006.01)

(21) International Application Number:
PCT/US2013/077348

(22) International Filing Date:
21 December 2013 (21.12.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
13/723,879 21 December 2012 (21.12.2012) US

(71) Applicant: **MICROSOFT CORPORATION** [US/US]; One Microsoft Way, Redmond, Washington 98052-6399 (US).

(72) Inventors: **LOFTUS, Jacob J.**; c/o Microsoft Corporation, LCA - International Patents, One Microsoft Way, Redmond, Washington 98052-6399 (US). **NAEHRIG, Michael**; c/o Microsoft Corporation, LCA - International Patents, One Microsoft Way, Redmond, Washington 98052-6399 (US). **BOS, Joppe Willem**; c/o Microsoft Corporation, LCA - International Patents, One Microsoft Way, Redmond, Washington 98052-6399 (US). **LAUTER, Kristin Estella**; c/o Microsoft Corporation, LCA - International Patents, One Microsoft Way, Redmond, Washington 98052-6399 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

[Continued on next page]

(54) Title: MANAGED SECURE COMPUTATIONS ON ENCRYPTED DATA

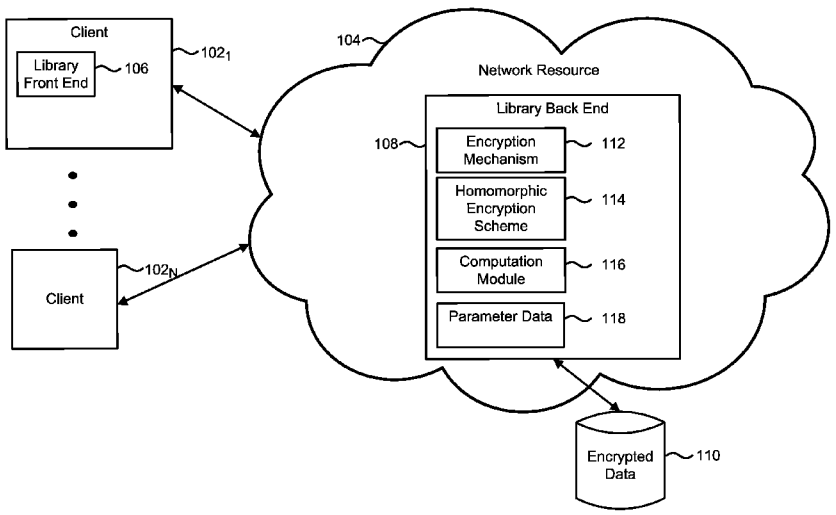

FIG. 1

(57) Abstract: The subject disclosure is directed towards secure computations of encrypted data over a network. In response to user desired security settings with respect to the encrypted data, software/hardware library components automatically select parameter data for configuring a fully homomorphic encryption scheme to secure the encrypted data items while executing a set of computational operations. A client initiates the set of computational operations via the library components and if requested, receives secure computation results in return.

WO 2014/100788 A3

WO 2014/100788 A3

Published:

— *with international search report (Art. 21(3))*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

(88) Date of publication of the international search report:
21 August 2014

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2013/077348

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/00
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2012/149395 A1 (IBM [US]; GENTRY CRAIG B [US]) 1 November 2012 (2012-11-01) abstract page 1, line 17 - page 5, line 13 page 13, line 20 - page 22, line 4 page 35, line 12 - page 46, line 27 page 59, line 1 - page 62, line 10 -----	1-5,9,10
X	CRAIG GENTRY ET AL: "Homomorphic Evaluation of the AES Circuit", 19 August 2012 (2012-08-19), ADVANCES IN CRYPTOLOGY CRYPTO 2012, SPRINGER BERLIN HEIDELBERG, BERLIN, HEIDELBERG, PAGE(S) 850 - 867, XP047013026, ISBN: 978-3-642-32008-8 the whole document -----	1-5,9,10
	-/--	

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 June 2014	30/06/2014

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Di Felice, M

2

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2013/077348

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

1-5

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-5

   A method of performing operations on data encrypted according to a homomorphic encryption scheme wherein parameters and configurations of said operations are determined automatically.

   ---

2. claims: 6-8

   A system for generating a set of keys from a truncated polynomial ring for use in a leveled homomorphic encryption scheme, wherein each element in a data set is mapped to a single element of the polynomial ring, and providing a computer device with homomorphic functions to use with the data set.

   ---

3. claims: 9, 10

   One or more computer-readable media for establishing a security parameter for a leveled fully homomorphic encryption scheme, encrypting data according to said scheme, computing an inherent noise estimate for each data item, and using a library to select an operation to perform.

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CRAIG GENTRY ET AL: "Better Bootstrapping in Fully Homomorphic Encryption", 21 May 2012 (2012-05-21), PUBLIC KEY CRYPTOGRAPHY PKC 2012, SPRINGER BERLIN HEIDELBERG, BERLIN, HEIDELBERG, PAGE(S) 1 - 16, XP047004400, ISBN: 978-3-642-30056-1 the whole document	1-5

X	ZVIKA BRAKERSKI ED - REIHANEH SAFAVI-NAINI ET AL: "Fully Homomorphic Encryption without Modulus Switching from Classical GapSVP", 19 August 2012 (2012-08-19), ADVANCES IN CRYPTOLOGY CRYPTO 2012, SPRINGER BERLIN HEIDELBERG, BERLIN, HEIDELBERG, PAGE(S) 868 - 886, XP047013028, ISBN: 978-3-642-32008-8 the whole document	1-5

A	BETLEY S ET AL: "The cyclotomic trace and curves on K-theory", TOPOLOGY, PERGAMON, vol. 44, no. 4, 1 July 2005 (2005-07-01), pages 845-874, XP027866140, ISSN: 0040-9383 [retrieved on 2005-07-01] the whole document	6-8

A	PETTER ANDREAS BERGH: "Ext-symmetry over quantum complete intersections", ARCHIV DER MATHEMATIK ; ARCHIVES MATHÉMATIQUES ARCHIVES OF MATHEMATICS, BIRKHÄUSER-VERLAG, BA, vol. 92, no. 6, 12 May 2009 (2009-05-12), pages 566-573, XP019699161, ISSN: 1420-8938 the whole document	6-8

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2013/077348

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2012149395 A1	01-11-2012	US 2013170640 A1	04-07-2013
		WO 2012149395 A1	01-11-2012